



# Physical **Red** Teaming for Cyber Security Teams

---

**Ana Aslanishvili & Shawn Abelson**

# Agenda

- ▶ Physical Security Primer for Cybersecurity Professionals
- ▶ Physical Red Teaming (PRT)
- ▶ PRT Approaches for Cybersecurity Teams
  - Similarities & Differences
- ▶ PRT Lifecycle
- ▶ Common Pitfalls of PRT (Learn from Our Mistakes)
  - Red Teams Gone Wild
- ▶ Becoming a Good Physical Red Teamer
- ▶ How to Run Physical Red Teams
- ▶ Contributing to the Profession
- ▶ Resources



# About Us

**PRM:** We conduct, build, and train red teams, helping organizations mature and improve security.

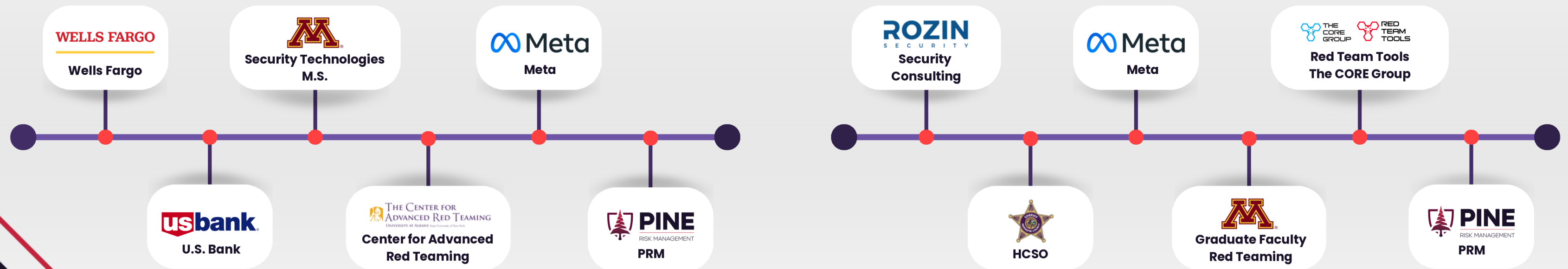
**Meta:** Started largest physical red team in Silicon Valley, hired dozens of testers, and built a team to oversee findings remediation across global office and data center footprint.



Ana



Shawn



# Physical Security @ Def Con

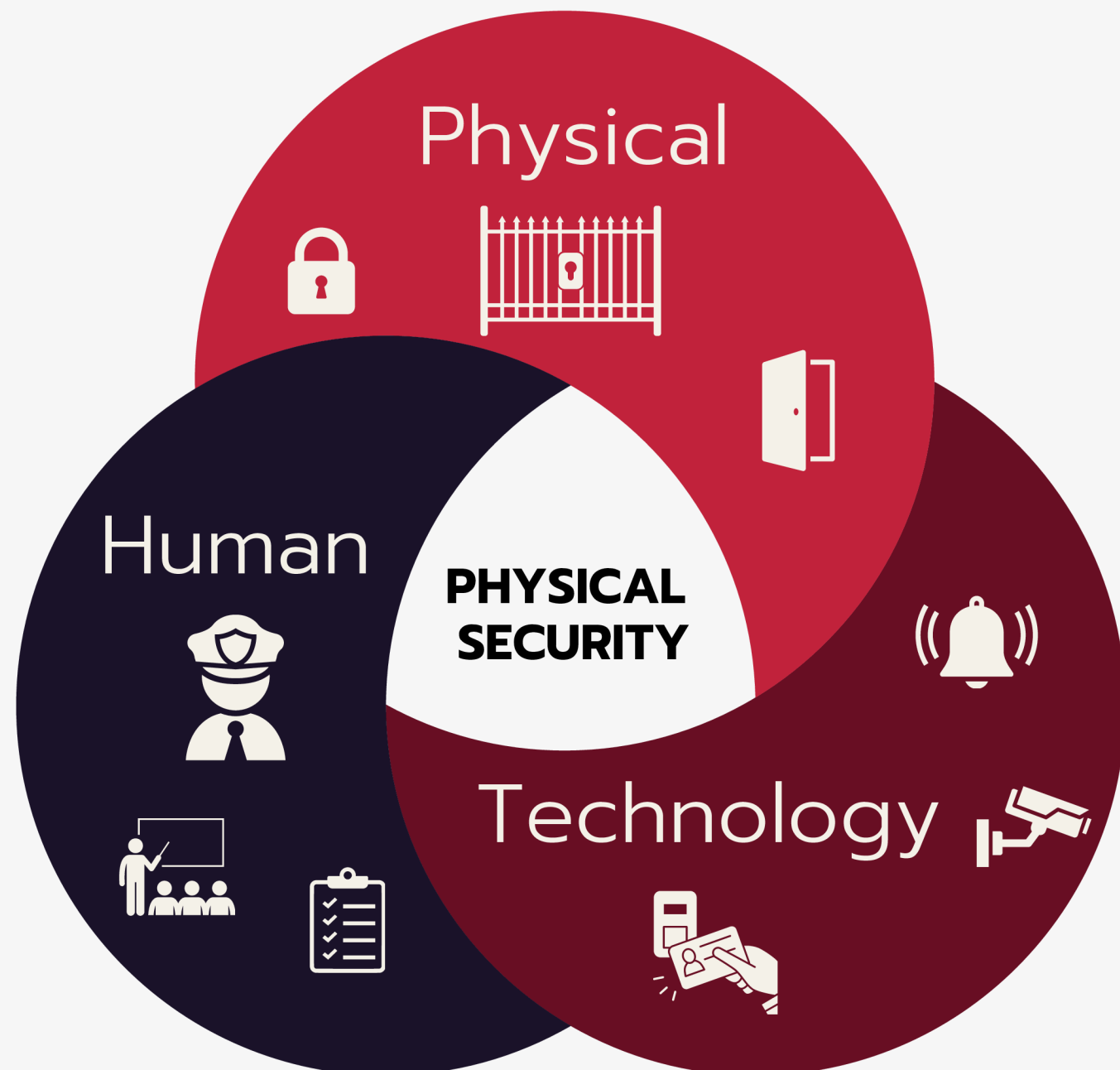


- 8/8: Red Team Alliance's Red Team Rendezvous
- 8/9: High Intensity Deconstruction: Chronicles of a Cryptographic Heist
- 8/9: Badge Cloning: A Penetration Tester's Guide to Capturing and Writing Badges
- 8/9: Physical Security - Bypassing Access Control Systems
- 8/9: Optical Espionage: Using Lasers to Hear Keystrokes Through Glass Windows
- 8/9: Master Splinter's initial physical access dojo: Storytelling of a complex adversarial
- 8/10: Physical Red Teaming for Offensive Cyber Teams
- 8/10: Improv and social engineering for red teamers
- 8/11: Physical OSINT
- 8/11: Fitness of Physical Red Teamers



# Physical Security

Protecting People, Assets, and Reputation. Security measures that deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm.



## Components of Physical Security

**Physical:** Doors, locks, gates, bollards, etc.

**Technology:** PACS, CCTV, Radios, Investigative, and Intelligence tools

**Human:** Guards, Analysts, Managers, Awareness, Processes & Procedures

# Physical Security

## Physical Security Teams & Activities



Threat Management



Event Security



Travel Safety



Business Continuity



Systems and Design



Quality Assurance



GSOC



Red Team



Investigations



Intellectual Property Protection



Supply Chain Security



Security Awareness



Insider threat management



Guard-force management



Governance, Risk, and Compliance



Audit



Protective Design



Resilience



Protective Intelligence



Executive Protection

& More 



# Physical Security

## Goals of Physical Security



Deter



Detect



Prevent  
Protect / Delay



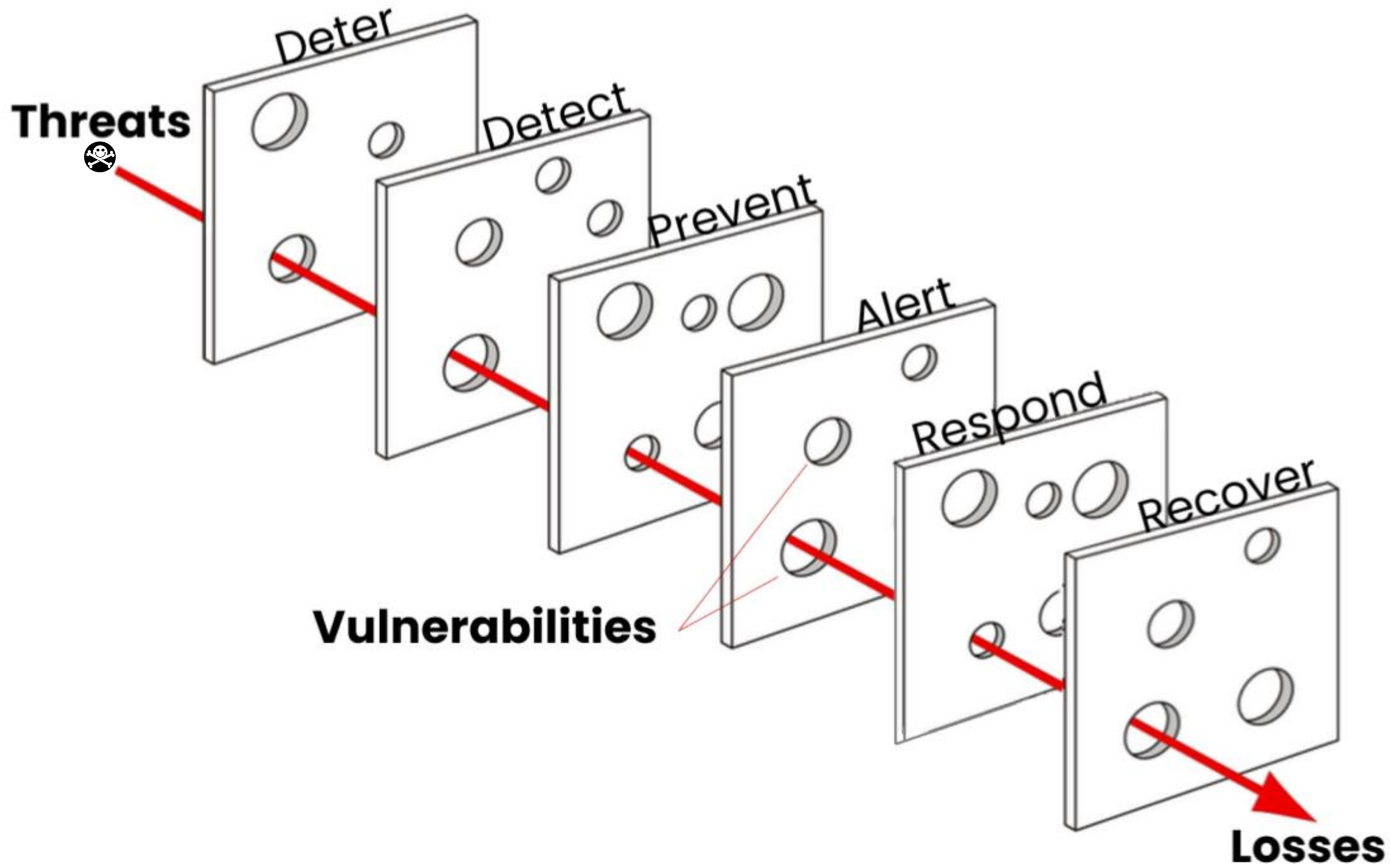
Alert



Respond



Recover







# Case Study

15 v 1

Radio Thefts,  
Bugs,  
and Foot Chases,  
Oh My



# The Profession of Physical Security

AMBIGUOUS BORDERS

VARIABLE REPORTING STRUCTURES

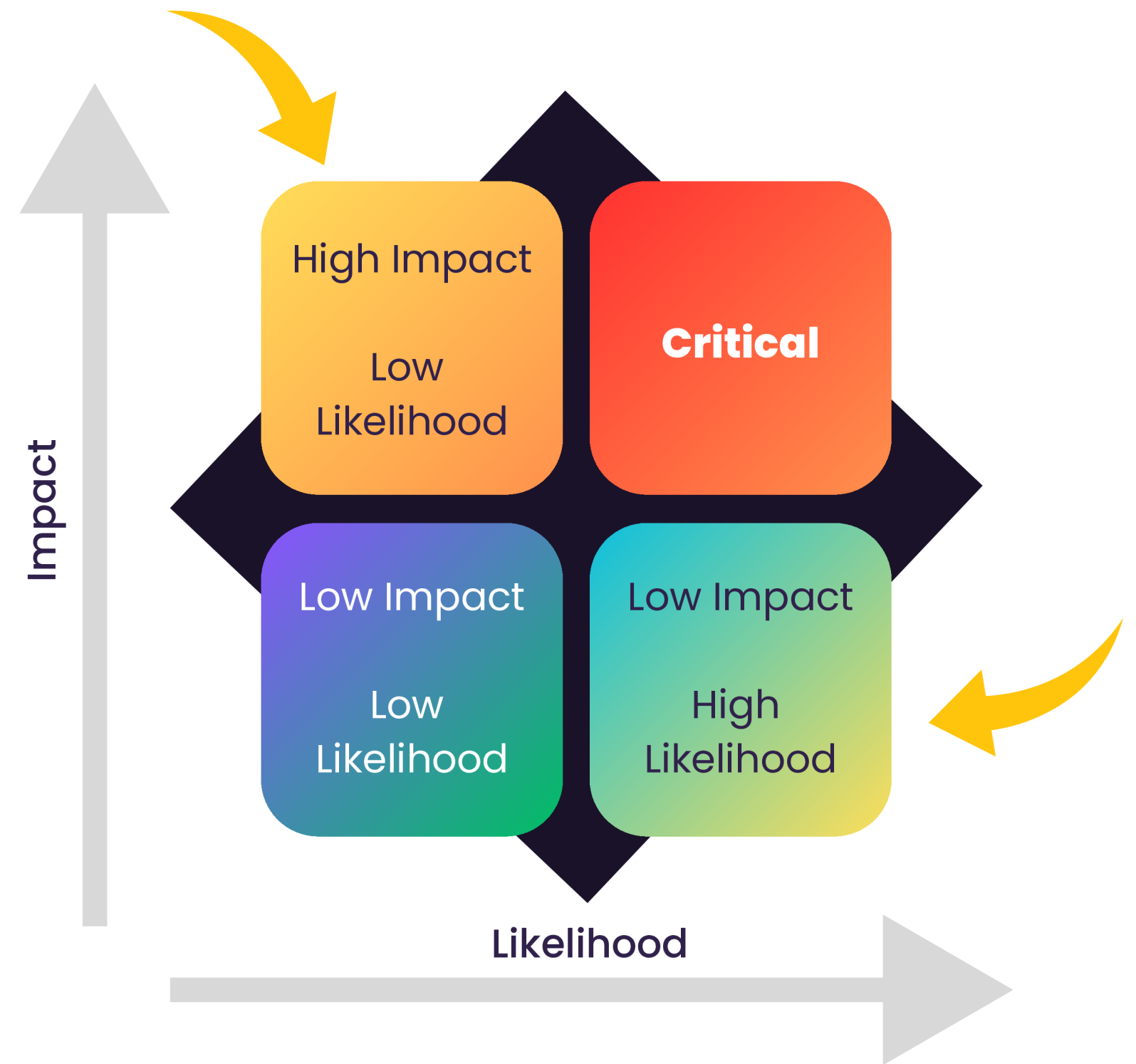
HIERARCHICAL

IMMATURE

SLOW

IRREGULAR

ASYMMETRIC





# Testing Physical Security

PHYSICAL SECURITY COVERS A WIDE ARRAY OF THREATS WITH A LIMITED BUDGET.

Infosec conducting Physical Security testing can result in a undue and overwhelming focus on technology and physical measures protecting IT infrastructure.

**Example:** Your testing may trigger a million dollar remediation project to replace Wiegand with OSDP, when in reality the likelihood of a badge being cloned is dramatically lower than that of workplace violence (domestic violence) or insider threat.

?

Some security programs are immature and need the help. Many are not and are drowning in data, threats, vulnerabilities, and more.



**Before you test, know how you will contribute to the status quo and prioritization.**

# Define **Red** Teaming

Stress Testing:

Testing a system with the goal to improve it



## Types of **Red** Teams

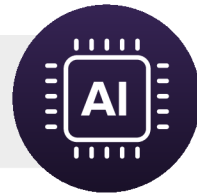
CYBERSECURITY



PHYSICAL SECURITY



AI



ANALYTICAL **RED** TEAMING



PRIVACY



## Types of Assessments

ASSET FOCUSED  
ASSESSMENT



VULNERABILITY FOCUSED  
ASSESSMENT



THREAT FOCUSED  
ASSESSMENT



# Define Red Teaming

## WHAT'S THE POINT?

The Red Team as a Blue Team in disguise.

*Red Team findings help the Blue Team prioritize the endless litany of tasks, fixes, and remediations they need to accomplish - driven by the same purpose behind the mission.*

### Threat-Centric Risk Framework

**Focus:** Profiles probable attackers and their likely methods of attack.  
**Approach:** Identifies avenues of attack and the targeted hardware/software.

Figure out who will target you, put yourself in their shoes and figure out their target: TTPs, vulnerabilities they may exploit, etc.

### Vulnerability-Centric Risk Framework

**Focus:** Identifies security vulnerabilities within the system.  
**Approach:** Quantifies the criticality of each vulnerability.

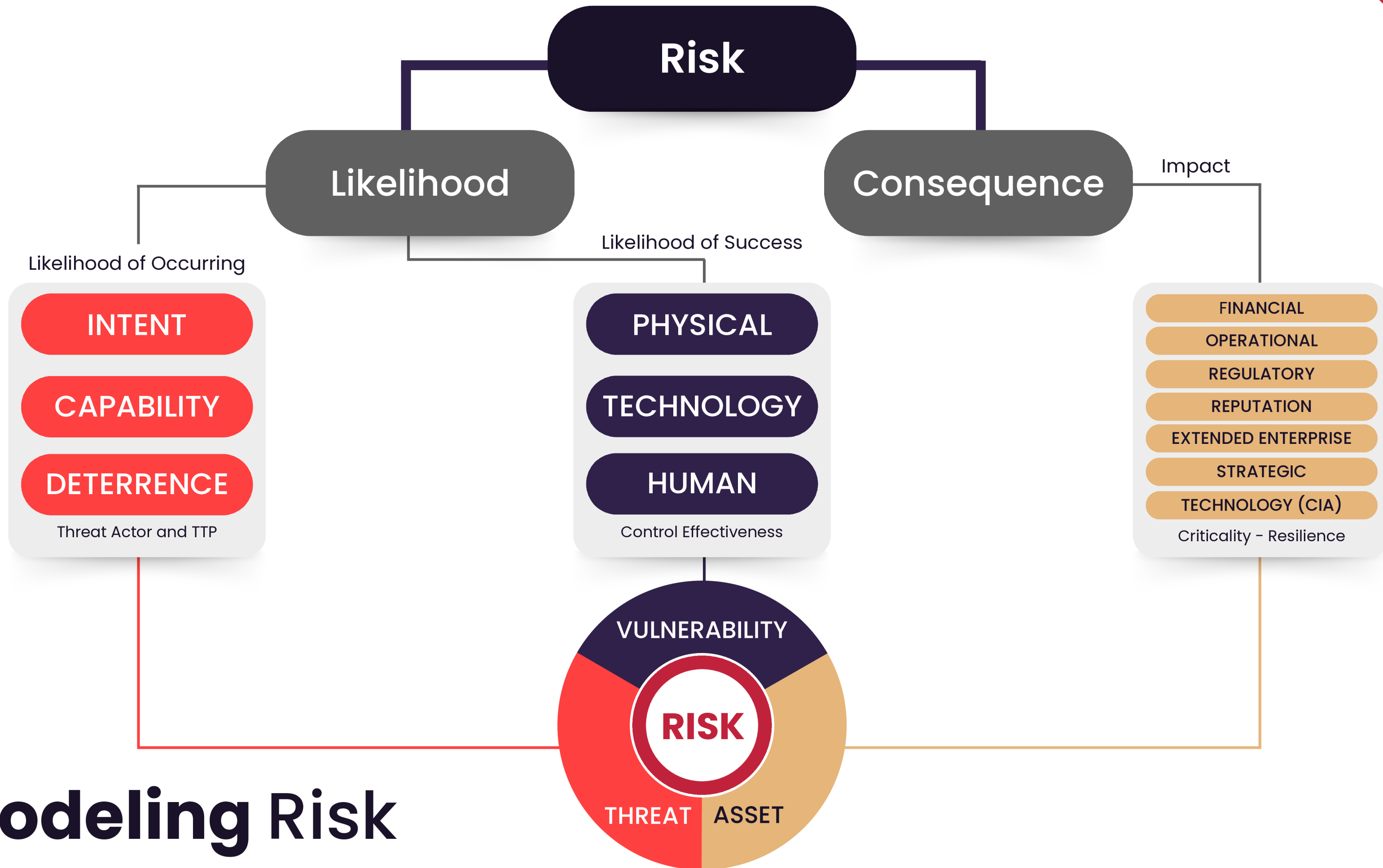
Testing of specific controls to validate strength, identify weaknesses, and improve capabilities.  
Pen Testing.

### Asset-Centric Risk Framework

**Focus:** Identifies and prioritizes risks based on system assets.  
**Approach:** Evaluates the business impact of losing each asset.

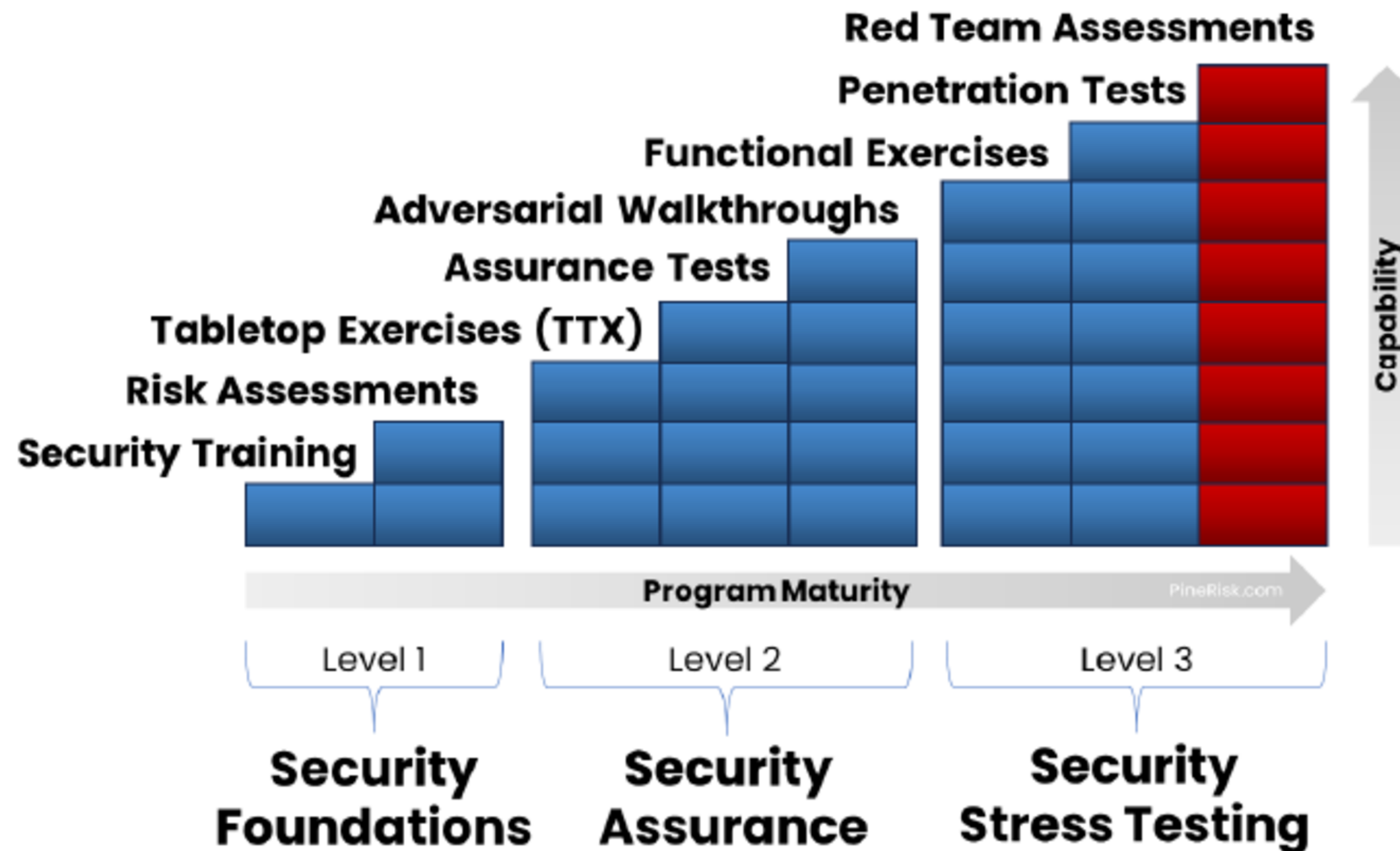
Identify the business's goals, and the most important assets that enable those goals to succeed.  
Steal the Assets.

# Modeling Risk



# Physical Red Teaming

## Security Maturity Spectrum



# Why are Cybersecurity teams testing Physical Security?



Cyber teams testing whether physical security creates cyber weaknesses



Cyber teams testing physical because it's fun & interesting



Cyber teams partnering with physical to help improve physical programs



Cyber teams testing physical as part of a requirement (certification or regulatory)



# Approach: Team Makeup

WHAT TYPE OF TEST ARE YOU RUNNING?

**Physical Enabled  
Cyber**



**Full Physical  
Assessment**



**Cyber with  
a Twist**



**Test Specific  
Physical Controls**



**Test Physical  
Security Technology**



# Benefits of Testing Physical Security

**1** **Breakdown Boundaries / Silos**

- Don't give the adversary an advantage

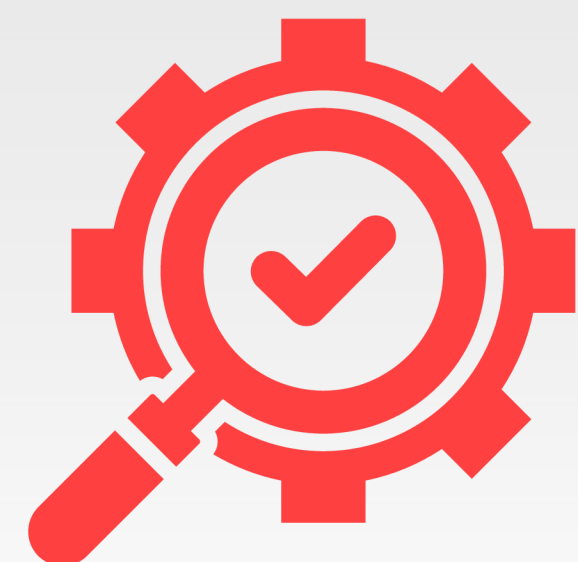
**4** **Increased Collaboration between Physical / Cyber**

**2** **Holistic View of Company's Security Risks**

**5** **Better Assessments**

**3** **Unassigned Areas of Responsibility**

- Fiber-tapping
- Vendor Onboarding
- Insider Threat





# Similarities in Testing

Approach – Adversary emulation / stress testing  
 Need for OpSec  
 Blue teamer in disguise  
 Kill-Chain

Security Objective	Prevent	Security Component	Human	Security Layer	Roof Access								
Recon	Surveillance	Resource Development	Probing	Perimeter Breach	Facility Breach	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Exfiltration	Impact	
54 Techniques	17 Techniques	22 Techniques	44 Techniques	33 Techniques	37 Techniques	44 Techniques	52 Techniques	26 Techniques	32 Techniques	24 Techniques	46 Techniques	43 Techniques	34 Techniques
OSINT	Identify Security Measures	Impersonation	Testing physical barriers and locks	Posing as maintenance or repair personnel	Climbing fences or walls	Using stolen or counterfeit access cards	Creating hidden compartments within the facility	Using stolen or forged credentials	Disabling security cameras or alarms	Mapping out security camera locations	Gathering sensitive documents or data	Smuggling documents or data out of the facility	Destroying physical security systems or barriers
OSINT	Individual Dynamic Surveillance (walking around)	Probing	Attempting to access restricted areas	Using fake identities to gain information	Cutting through barriers or fencing	Tapping authorized personnel into buildings	Installing covert surveillance equipment	Exploiting software vulnerabilities	Using counterfeit identification	Identifying access control points	Recording audio or video of sensitive areas	Using encrypted communication channels	Tampering with critical infrastructure
OSINT	Vehicle-Based Surveillance	Probing	Conducting false maintenance requests	Pretending to be a new employee	Using vehicles to ram gates or barriers	Posing as cleaning or maintenance staff	Placing devices that can be remotely accessed	Manipulating access control systems	Erasing or manipulating logs	Surveying internal layout of the facility	Using covert cameras or recording devices	Transferring data to external storage devices	Disabling power or communication lines
OSINT	Localized Image Search	Probing	Checking for unsecured doors or windows	Conducting false maintenance requests	Using lockers or other tools to scale obstacles	Forcing doors or windows open	Using social engineering to gain higher privileges	Disrupting an authorized personnel	Utilizing insider knowledge to avoid detection	Gathering employee shift schedules	Collecting access credentials and badges	Sending data via email or file sharing services	Initiating fire or smoke to cause confusion
OSINT	Obtain Facility Layout	Probing	Using social engineering to gather access information	Posing as law enforcement or government officials	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Hiding in seldom-used areas of the facility	Compromising administrator accounts	Using encryption to hide activities	Identifying key personnel and their routines	Harvesting information from unlocked computers	Using remote access tools for data transfer	Damaging key assets or equipment
OSINT	City construction permits	Probing	Using social engineering to bypass security systems	Clearing and testing security personnel reactions	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	City blueprints	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Searching for unsecured or less-secured areas	Collecting discarded documents from trash or recycling	Uploading data to cloud storage services	Introducing malware or ransomware
OSINT	Landlord retail site	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Identify Vendors	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Observation of site layout and security features	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Questioning employees about site operations	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Identify security camera locations	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Recording entry and exit points	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Mapping out patrol routes	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Identifying blind spots in surveillance coverage	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Using drones for aerial surveillance	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Monitoring delivery and service schedules	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Checking for public Wi-Fi networks	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Social engineering attempts to gather information	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Identifying security weaknesses through social media	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Watching for security drills and security response times	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Taking photographs of critical infrastructure	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Using binoculars or long-range cameras	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Observing access control procedures	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Monitoring security checkpoints	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability
OSINT	Surveilling parking lot usage patterns	Probing	Using social engineering to gather access information	Using social media profiles to gain trust	Using lockers or other tools to scale obstacles	Exploiting HVAC or utility access points	Setting up temporary camps or stations	Utilizing insider threats or collusion	Disrupting security protocols or detection tools	Analyzing entry and exit logs	Obtaining data from printers or servers	Concealing data within other files or images	Compromising data integrity or availability

# Dissimilarities in Testing



**VULNERABILITY  
PATCHING**



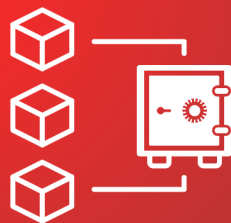
**CIA VS. DEATH AND CUSTOMER  
SERVICE**



**CONSEQUENCES OF GETTING  
CAUGHT**



**STAKES CAN BE HIGHER FOR  
PHYSICAL TESTERS**



**LESS COMMON**

- Testing is Less Common
- Adversaries are Less Commonly in Person



**THIRD PARTIES ARE  
OFF-LIMITS**



**SOCIAL ENGINEERING**



# Guiding Principles

## LISTEN

Talk to CSO/CISO/CTO, and whoever physical security reports to



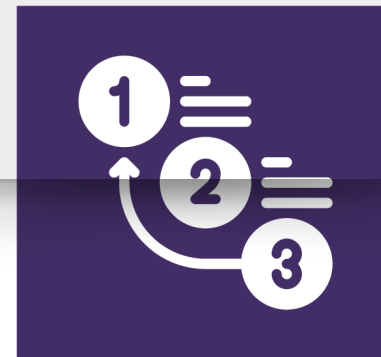
## UNDERSTAND

The business. Where are the risks, and where would good data help with decision making?



## PRIORITIZE

Based on the threat model and decisions that leadership needs to make



## SCOPE

Scope the engagement to meet the company's needs, partner with physical security, and reduce risk

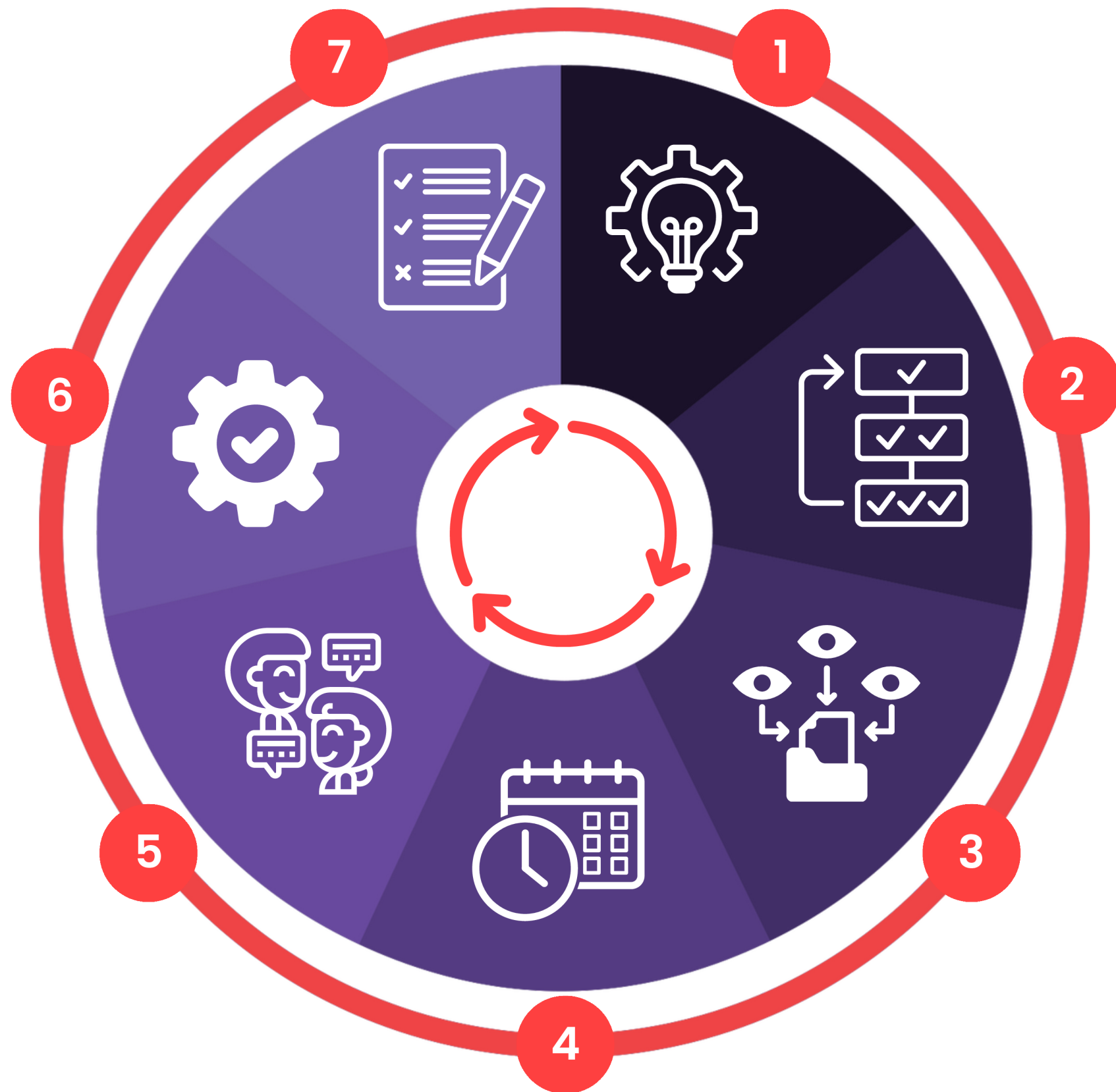


## HELP

Ensure you're helping the blue team. You are on their side.



# Red Team LifeCycle



- 1 IDEATION
- 2 PRIORITIZATION
- 3 INTEL GATHERING
- 4 PLANNING
- 5 REHEARSAL
- 6 EXECUTION
- 7 REPORTING

*remediation if you are a narc*



# 1 Threat Modeling > Ideation

Build and revisit your organization's threat model at least once a year for accuracy and relevancy

Account within it for external information only (the internal factors will come later) – this needs to be an objective resource based on true and verifiable intelligence



## Resource

[Threat Modeling Overview](#)

Basic Threat Modeling Visualization:

- [Standard](#)
- [Long](#)

## 2 Ideation > Prioritization

- ▶ **Poison Circles**
- ▶ **Stakeholder Interviews**
- ▶ **Insider knowledge, *if permitted***

Note that the specific use and extent of insider knowledge, if and when used, should be well-documented for reporting purposes (this can and will CYA on several occasions if you are anything like us).



# 3 Prioritization > Intel-Gathering



- ▶ OSINT
- ▶ Research
- ▶ Internal resources

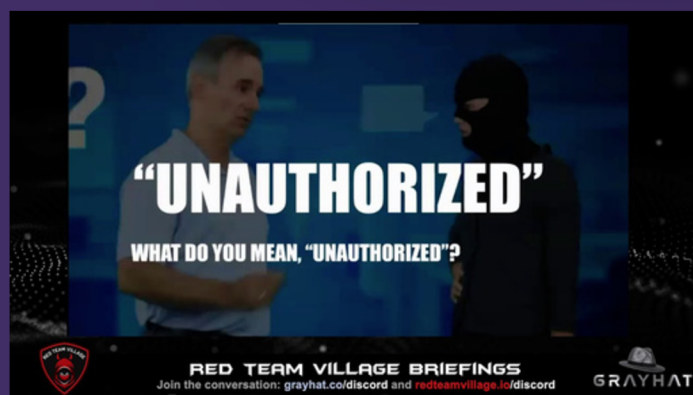
# OSINT for PhySec Red Teaming

## Building

- ▶ **Blueprints**
  - Tax Records for Building Owner
  - Building Manager
  - Leasing Office
  - City Records, Construction Permits
- ▶ **360 Tours**
  - Leasing Agents
- ▶ **Photos Inside**
  - Tags and Geolocation

## Routes In & Intel Gathering

- ▶ **Find Vendors**
  - Listed on their website
  - News articles
  - Purchase orders
  - Photos
  - [Surveillance / Probing]
- ▶ **Find Co-Tenants**
- ▶ **Find Empty Floors**
- ▶ **Crime Maps**
- ▶ **Wifi (WIGLE)**
- ▶ **Complaints and Neighborhood Conversations**
- ▶ **Employees (LinkedIn)**
  - Photos, Discussions, etc.



[Previous RTV Talk on OSINT for Physical](#)  
by Tim Roberts & Brent White



# 4 Intel-Gathering <> Planning



- ▶ Scope
- ▶ Comms
- ▶ OpSec
- ▶ Resource Acquisition
- ▶ De-Risking

## Resource

Red Team Scoping Questions

- START-Physical [Under Construction]

De-Risking the Red Team  
Letter of Authorization  
Template

# De-Risking

The goal of red teams is to reduce the risk to the organization, not to increase it. Ensure tests do not cause undue risk or disruption.

## Categories or Risk:

EHS, Legal, Privacy, Compliance, GSOC, Tenant/Landlord, Firearms/Weapons, Other Risks

## Key Question: Do you Notify Law Enforcement?

## Authorization Confirmation:

If you get caught, how do they confirm you are authorized?

## LoA, Phone Numbers, Internal Post/Page, Notification of LE

**Laws:** Review OpsPlan against local laws

**STOPOP:** When is the operation done? What are the triggers for stopping early?

## 5 Planning <> Rehearsal



- With the field info-gathering, the operators can start probing for next steps or more information as they progress.
- This new information should inform the next steps in the op.  
You receive pushback on vishing attempt but learn an additional step of the authentication process that sets you up for success for the next call.
- Rehearsal is a must for op success when using social engineering tactics, so practice vishing conversations and scenario building. But it's pivotal for physical exploits involving any danger to the operator or others, such as fence-climbing, badge-swiping, and more

## 6 Rehearsal <> Execution

Leverage all knowledge from OSINT-gathering, surveillance, and probing to make your execution a success. it's a cyclical process.

**Strong communication**

**Goal Focused**



## 7 Execution > Reporting

After the execution follows the most loved portion for any operator – riveting report-writing!

It's important to remember that as a red teamer **you are on the same team as the rest of the organization.** Your job is to help them redirect and prioritize their remediation efforts.



# Common Pitfalls

## DON'T:

Cause or use uncomfortable social topics to gain entry (race, gender, etc.)



Create more risk than you mitigate



Bring your Politics to Red Teaming



Commit Crimes (you're authorized, or not)



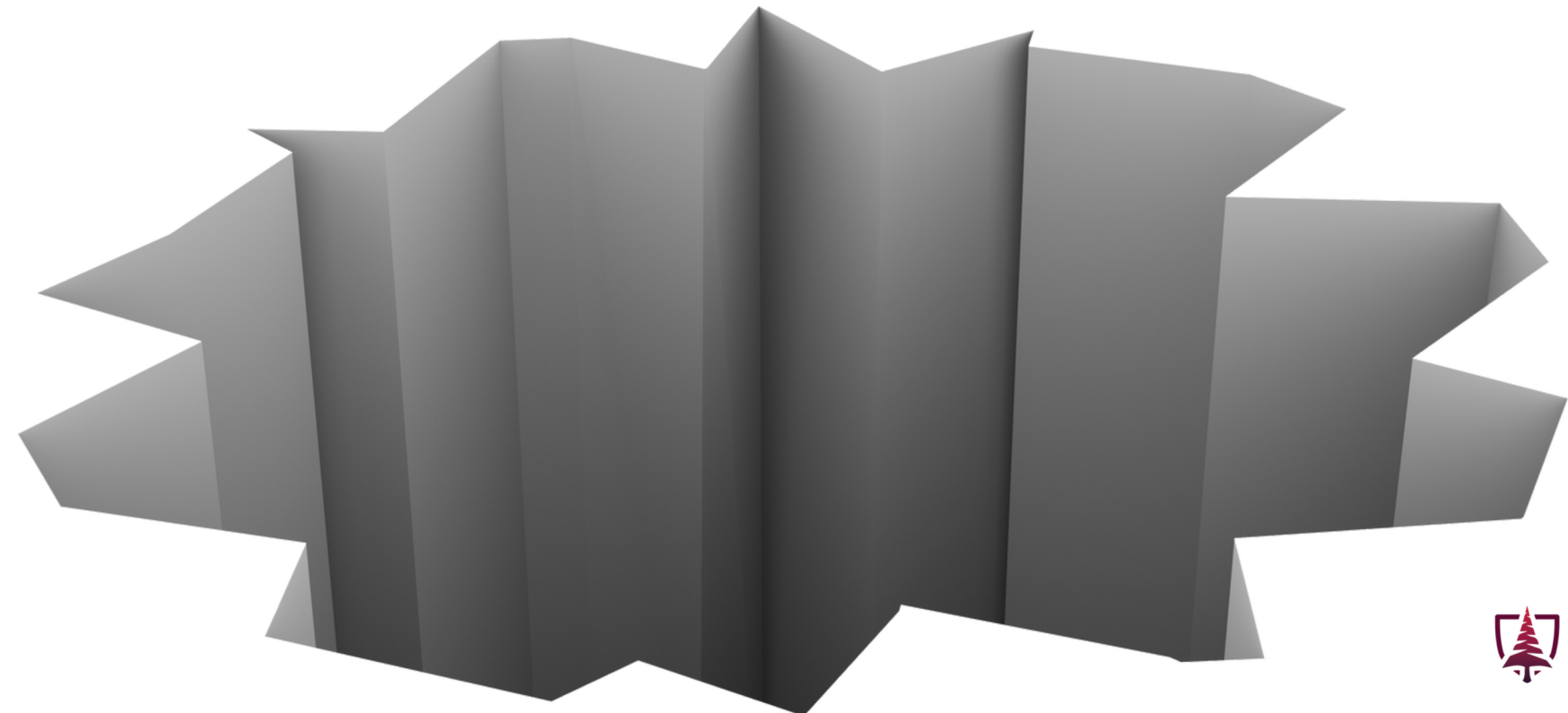
Steamroll



Brag (Afterward or outside of reporting chain)



Do Cowboy Shit





# The Don't of Physical Red Teaming

## DON'T:

Create vulnerabilities and leave them  
(even if the client says it's ok)



Break into the wrong floor



Accidentally Assault Someone



Reach for your LoA in your back pocket  
while a cop points an AR15 at you



Get anyone fired



Pay or take bribes



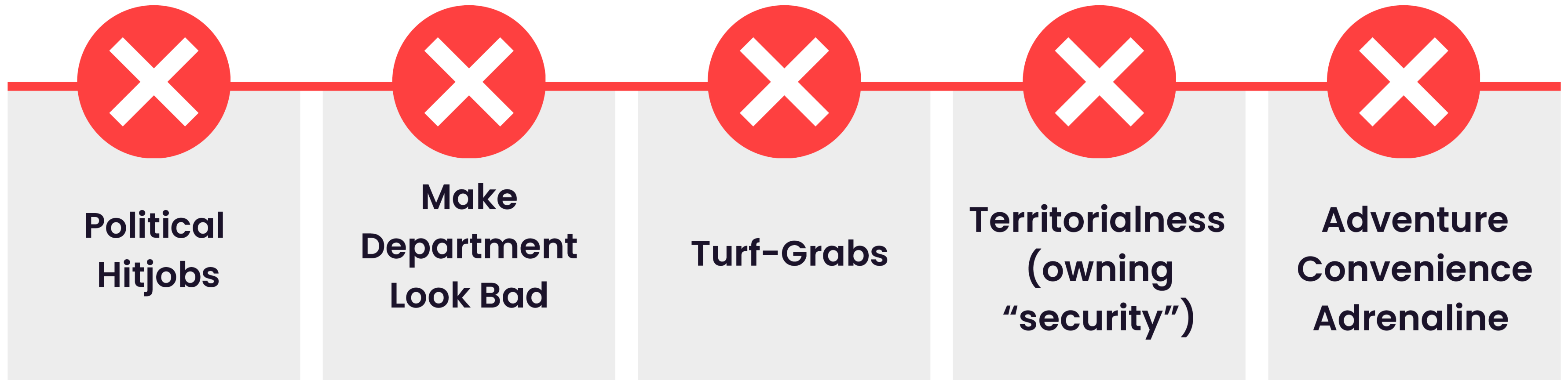
Use a fake Letter of Authorization (Get out  
of Jail Free card)



Make security's job harder



# Bad Reasons to Conduct Physical Assessments





# Physical Red Teams

## Gone Wrong

- Helicopter
- Long Guns
- Special Delivery
- Fire Alarms
- Steamroller
- Tel Aviv

### Resource

▶ [Physical Red Team Lessons Learned](#)



# What makes a good physical red teamer?

## Step 1: Fundamentals

- The Mindset: What is **red** teaming?
- The basics of physical security
- Analytical Red Teaming
- Cyber Red Teaming



## Step 2: Technical Skills

- Social Engineering
- OSINT
- PACS
- Bypass Techniques
  - Lockpicking

## Step 3: Professional Skills

- Systems Thinking
- Ethics & Laws
- Red Teams Gone Wrong
- Managing Red Team Risk
  - Effective Scoping
- Learning from the real Baddies (Effective Threat Modeling & Adversary Emulation)
- Security Frameworks, Standards, and Regulations
- Report Writing and Impactful Communication

## Resource

Breaking into Red Teaming - Overview

[Part 1 - Fundamentals](#)

[Part 2 - Technical Skills](#)

[Part 3 - Professional Skills](#)

[▶ Physical Red Teaming Ethics Scenarios](#)

# Building the Team

**PICK YOUR POISON:**

**Lockpicking**

**Social  
Engineering**

**Impersonation**

**OSINT**

**Bypass  
Techniques**

**RFID/PACS  
Hacking**

**Fence  
Jumping**

**Tailgating**

**More**

You don't have to be great at any of these – just adequate. If you're testing against an advanced insider threat or counterintelligence team, you need to be great. Otherwise, be decent at half of them AND have good professional skills.



# Let's Get Physical

Seven Steps for Cyber Teams to Conduct Good Physical Assessments

## TALK

Talk to the Physical Security Teams Early



## UNDERSTAND

Understand their needs, strengths, known weaknesses, goals, etc.



## SCOPE

Focus on objectives



## DE-RISK

Get Authorization



## COMMUNICATE

Before, during, and after with all parties



## DEBRIEF

Show & Tell



## FRAMING

Present, frame, and communicate your findings effectively. Know your audience. Technical terms don't work, pose it in terms of risk, threat model, and threat actors. They don't know what APTs are targeting your networks, so use the data you have to tell a compelling story.



# Collaborating with PhySec



## THREAT IDEATION:

Poison Circles



## PHYSICAL-ENABLED CYBER VULNERABILITY SHARING

(If someone gets into an IDF room, X happens. If someone gets access to a LAN port on a wall in the office, Y happens). Let them know your strengths and weaknesses.

## JOINT OPERATIONS:

Pull their folks into your assessment if you need a physical component



## INFORM RISK ASSESSMENTS



## JOINT TRAINING



## OVERLAP



# Unintended Benefits of PhySec Testing



Where's Waldo  
badge spotting

Increased  
vigilance

Lower bar for  
reporting  
suspicious activity





# How PRT Saves Money



## Test Efficacy of Completed Projects



## Uncover Gaps in Vendor Implementation



Loss Avoidance:  
Avoidance of loss of assets,  
negligence lawsuits, etc.

Insurance – Tangible &  
Tested Risk  
Reduction

Removal of Ineffective  
Technology

Risk  
Acceptance

Challenging Assumptions  
Cameras in Office Space

# Contribute to the Industry

Physical Security is relatively immature


Physical red teaming is even less mature as a profession


## IF YOU WANT TO CONTRIBUTE:

Publish stories, write frameworks, give talks. 

Develop tools, Open Source Them. 

### **Learn about Physical Security:**

Go to a conference, take a course, and translate it to Cybersecurity professionals. 

Take effective and mature aspects of the cybersecurity and try applying them to physical security. 

# Resources

## Locks & Leaks

[locksandleaks.substack.com](https://locksandleaks.substack.com)



## Red Team Tools

[www.redteamtools.com](https://www.redteamtools.com)



## Resources From This Talk

[www.pinerisk.com/RTV](https://www.pinerisk.com/RTV)



## Red Team Alliance

[shop.redteamalliance.com](https://shop.redteamalliance.com)



# Thank You!

## Get in Touch



Text/Call: (628) 777-7475  
Signal: (952) 465-4769



Shawn@PineRisk.com  
Ana@PineRisk.com



Reddit.com/r/PhysicalRedTeam  
Discord: ByteAbel  
LinkedIn.com/Company/PineRisk

